World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:14, No:11, 2020

A Socio-Technical Approach to Cyber-Risk Assessment

Authors : Kitty Kioskli, Nineta Polemi

Abstract : Evaluating the levels of cyber-security risks within an enterprise is most important in protecting its information system, services and all its digital assets against security incidents (e.g. accidents, malicious acts, massive cyber-attacks). The existing risk assessment methodologies (e.g. eBIOS, OCTAVE, CRAMM, NIST-800) adopt a technical approach considering as attack factors only the capability, intention and target of the attacker, and not paying attention to the attacker’s psychological profile and personality traits. In this paper, a socio-technical approach is proposed in cyber risk assessment, in order to achieve more realistic risk estimates by considering the personality traits of the attackers. In particular, based upon principles from investigative psychology and behavioural science, a multi-dimensional, extended, quantifiable model for an attacker’s profile is developed, which becomes an additional factor in the cyber risk level calculation.

Keywords : attacker, behavioural models, cyber risk assessment, cybersecurity, human factors, investigative psychology, ISO27001, ISO27005
Conference Title : ICCSITCSRA 2020 : International Conference on Cyber Security for Internet of Things, Cyber Security Risk and Analytics
Conference Location : Amsterdam, Netherlands
Conference Dates : November 05-06, 2020